Winter 12-5-2004

Customers Confidence in E-Business: An Evaluation of Australian Practices A Case Study

Daniel Chandran

Customers Confidence in E-Business: An Evaluation of Australian Practices A Case Study

Daniel Chandran

Faculty of Information Technology, University of Technology, Sydney, Australia
noble@it.uts.edu.au

ABSTRACT

Many Internet users perceive that there is a large risk to their privacy and security when they buy products and services or submit personal information online. Although the perception of risk may be greater than the actual risk, it is still a cause for concern. An e-business must address customers' perceived risk just as much as any actual risks. In other words, the issue of trust is fundamental as security and privacy issues are of major concern for many users. Customers are looking for security policies and procedures businesses are implementing and their responsibilities in keeping customer information secure.

This paper deals with trust e-businesses can create through their websites. A comprehensive set of criteria had been used to evaluate Web sources with a high level of meticulousness. Criteria include accuracy, authority, currency, scope, and relevance. A methodology has been developed and two main industries actively operating in e-business within Australia, namely, the Banking and Retail industries have been chosen. Under each industry, two businesses were identified and sources evaluated. It is presumed that using such criteria would help to gain customers confidence. Findings are reported.

Keywords: e-commerce, Privacy and Security, Trust, Evaluation Criteria.

1. INTRODUCTION

The Internet provides instant and universal access to a range of business sites. Any business that offers services through the Internet needs to be concerned about network security as it is being constantly attacked. A computer network system is exposed to potential threats from anywhere on the public network. Businesses need to protect against such threats and implement stringent security measures. Many Internet users perceive that there is a large risk to their privacy and security when they buy products and services or submit personal information online. Although the perception of risk may be greater than the actual risk, it is still an issue for concern. An e-business must address customers' perceived risk just as much as any actual risks. From the point of customers, they are concerned about the hackers who can gain access to steal their information.

Trust can be defined as faith or confidence in a person or organisation. The level of security depends on the nature of business and the risks involved. For example, a web site providing information on the products of a company may not require the same level of security as an online banking Website. An e-business must identify the security issues that would provide the business more confidence and better relationship among its customers.

In the last few years, e-commerce went through difficult path of decline. One of the reasons is that the customers were not sure about the design and security holes. E-business in Australia is widespread and delivering benefits to the national economy. This paper is written from the customers' point of view and tries to list the ways through which the customers can evaluate the sources in terms of security and privacy before they can conduct any business online. Some frequently asked questions are:

- How is the data protected once it is delivered to the e-business?
- How are credit card transactions authenticated and authorized?
- Can I trust this Website?
- How can I best evaluate e-business information provided on the Internet?

When the customers are satisfied with the security measures provided by the business, they make frequent return visits to the web site or make repeat purchases from the web site. If they are not confident about the policies, the situation could change. Several customers research about a product on the website and purchase it offline. Customers may not understand the security policies described in the websites. In such a situation, how can they come to a conclusion whether a particular site is secure? It is important that users undertake a systematic approach to select sources, which they consider as secure. To exchange information through the use of technology, we must be certain that it is as safe as exchanging information face-to-face. In this study, numerous web searches were carried out to gather and select sources pertaining to businesses that offer online business in Australia and the information they provide to their customers.

A range of measures is required to inculcate confidence in customers to conduct business over the Internet.

Customers may have to evaluate sources with a high level of meticulousness, by using a comprehensive set of criteria. Criteria include Accuracy, Authority, Currency, Scope, and relevance. A methodology has been developed for this research and two main industries actively operating in e-business within Australia, namely, the Banking, and Retail industries identified. Under each category, two businesses were chosen and the sources evaluated. It is presumed that using such a set of criteria would help customers to gain confidence to choose and use a web site. Findings are reported.

2. AUSTRALIAN INTERNET USAGES

The intensity of Internet use by Australians is among the highest in the world. Australia ranks sixth in the world in terms of the total number of Internet users, despite its relatively small population (4). At the end of September 2003, total Internet subscribers in Australia numbered over 5.2 million, an increase of 135,000 (3%) from the end of March 2003. This modest increase follows the larger increases recorded in the previous two collections, 11% at the end of March 2003 and 8% at the end of September 2002. Majority of these were in the household market with over 3.9 million subscribers. Every second household has home Internet access. (5,9). Australian businesses earned A$43 billion (USD24 billion) in online revenue from December 2000 to mid 2002 (5).

Australian firms using e-business are saving between one to five percent of ongoing costs, while 10 percent of the businesses save 15 percent or more. (*Allen Consulting Group, Built for Businesses, Australia's Internet Economy, June 2001*). Online purchases of Web services such as recruiting and banking are becoming increasingly popular. (*NUA Internet Surveys, 26 July 2002).* Australian B2B e-commerce transactions were worth $6.2 billion in 2001 and likely to rise to $87 billion by 2006 (*International Data Corporation March 2002 Report "Australia B2B eCommerce forecast, 2001-2006).* At the end of March 2002, the number of registered online banking users almost doubled to reach 5.23 million, up from 2.77 million in 2001. The total number of online transactions for the quarter ending March 2002 was 64.3 million, up 7 percent on quarter 1 of 2001 (*NUA Internet Surveys, 10 July 2002).* Usage of Internet banking has grown up to 36 percent in June 2003 from 15 percent in December 2000. Purchasing goods and services increased by 4 per cent in June 2003 compared to 2000.(10).

Australian businesses and IT leaders representing medium and large organisations rate security as either "very important" or "important". IDC Survey reports, Governments, business and individuals are moving forward with a heightened sense of security and the inherent interdependent responsibilities. The study also revealed that investment in IT security is increasingly being driven by strategic initiatives and less in response to security breaches to the organisation. Key drivers behind IT security investment are (i) Increased Internet and Intranet usage and (ii) Mobile computing

3. SECURITY STANDARDS AND POLICIES

The importance of security standardization and certification for e-commerce industry remains an important issue for businesses intending to conduct e-commerce over the Internet. Implementation of security systems must address threats on an ongoing basis. Standard security practices like ISO 17799 and AS/NZS/BS-7799 are used to prevent, detect and contain security breaches and obtain compliance certification. These standards cover critical aspects of good organisational security, which contains a comprehensive set of security controls to improve the level of security within any organisation. The standard is based on assuring integrity, availability, and confidentiality of information assets.

Security is not just the technology alone, but also having solid security policies and following ideal security practices. Without clear standard security policies and practices, e-commerce organisations will not be able to gain the trust of customers or business partners. Therefore the security needs will have to be provided as a set of centralized managed services ensuring corporate interface and information protection. As the e-commerce industry expands, the demands on security level also increases. Business requirements for security changes and the control to threats have to be addressed. It is better to utilise an approach based upon best practices, which has some form of track record, to prevent, detect and contain security breaches. Some security standards in practice serve as a single reference point for identifying a range of controls needed for most situations where information systems are used in industry and commerce.

The author experienced some limitations in gathering information relating to security breaches occurred due to security safeguards and inadequate security management. Hence, it is not possible to document specific scenarios and the measures taken to overcome such breaches. Data is collected through interviews, business websites, publications/white papers related to the issues concerning security and privacy. Though organisations are not willing to reveal previous security breaches, one could see the number of changes introduced in the security issues in the last few years.

4. EVALUATION METHODOLOGY

The triangular relationship between customer, e-business and data security is very simple and clear. In order to safely conduct business and exchange information through the use of technology, we still must be certain that it is as safe as exchanging information

face-to-face. As data loss and breach of privacy are serious concerns in e-trade, it is necessary for the customers to apply a few criteria to evaluate sources to reduce the risk of loosing valuable information. In this paper, the author identified specific areas in e-business and evaluated the contents of these web sites. The study also helped in getting a broader understanding of data security adopted by businesses in Australia.

4.1 Methodology

- Defining the task
- Selecting known businesses within the industries chosen
- Selecting a set of criteria for evaluation
- Evaluating the sources using the criteria
- Writing a conclusive statement using the information gathered

4.2 Defining the Task

To locate information, two types of industries actively operating in e-business, have been identified. They are

1. *Banking industry* - for its necessity of state-of-the-art security in all online transactions/transmissions
2. *Retail industry* – as it tends to operate on a smaller scale, and generally assumed to have less security.

4.3 Selecting businesses within the industries chosen

Two major banks in Australia, namely, *Westpac Banking Corporation and Commonwealth Bank of Australia* were chosen for the Banking Industry. For Retail Industry, *Woolworths Home Shop*, a major super market and *Roses Only*, a leading online florist, were chosen.

4.4 Selecting criteria to evaluate potential sources

The Three Basic criteria chosen to evaluate information security in e-commerce industry are:

- Confidentiality
- Integrity
- Availability

Confidentiality is ensuring that information is accessible only to those who are authorized to have access. Integrity is ensuring accurate, reliable and complete information protected from unauthorized alteration; and Availability is assuring information and associated assets accessible only to authorized users.

The above three criteria further elaborated into:

Criteria	Explanation
Relevance	How is this relevant to data security in eBusiness
Authority	Where is this information coming from?
Currency	When was this information published/updated? What has changed since this was published?
Scope	Does the information cover all aspects of Security issues? To what detail are aspects of this covered?
Accuracy	How accurate is the information provided? Can it be verified?

5. SOURCE EVALUATION

5.1 Banking Industry

Criteria	Westpac	Commonwealth Bank of Australia
Relevance	The policy states, "We are committed to protecting and maintaining the privacy, accuracy and security of your personal and financial information". Uses up-to-date and secure technology methods to protect information online using multiple firewalls, secure passwords and sign in processes. Personal information is passed through secure server using encryption technology. The site provides a guarantee "when you use Internet Banking, you can be confidant that we employ the highest level of security to protect your accounts and personal information". To confirm that the data is encrypted, a symbol of a lock appears at the bottom.	The Bank takes care of the protection of customers' information and transaction instructions seriously. As part of maintaining the highest level of customer service, the Commonwealth Bank has implemented system security controls, encryption of sensitive data and regular security reviews as well as a five minute time-out on **Net** Bank to avoid anyone else accessing your banking details on your computer. Net Bank assures the customers of safety, security, privacy and protection. "We guarantee it!" This means that the customers will not be liable for any unauthorised transaction as a result of using **Net**Bank. It uses 128-bit encryption of all customer data. Customers use Individual Client Numbers and Passwords. The Commonwealth Bank engaged Admiral Computing (Australia) to independently assess the security measures the Commonwealth Bank developed.
Authority	It is found in its official Website: www.westpac.com.au	**Issued by**: Commonwealth Bank of Australia ABN 48 123 123 124, www**.** commbank.com.au
Currency	Current. The Website is committed to bring	Current. Electronic Banking Product Disclosure

	customers up to date on the latest security features of online banking.	Statement Date: 5 February 2004
Scope	Describes security features extensively. The security section gives detail information on how to "protect yourself while banking online.". It also provides latest news on fraud issues, online security and safeguarding customer computer.	*Security and Privacy Statement* explains how customers' personal information will be treated as they access and interact with the Web Site. Information covers aspects of security, information collection and handling, how a breach could happen and how to prevent it.
Accuracy	"*Ask Westpac*" provides answers to questions about its products or services.	The Support Centre answers fAQs. Customers are further supported by **Net**Bank Help Desk on **13 2828.**

5.2 Retail Industry

Criteria	Woolworths	Roses only
Relevance	First level of security is customers login into Woolworths HomeShop with a username and password. Assures that the username and password are examined in a secure session and cannot be accessed by anyone else. This is the second level of security. While browsing around the shopping aisles, no secure data is being passed around and while checking out of the supermarket, another secure session allowing the purchase process to happen safely and privately. It uses the Secure Sockets Layer (SSL). This ensures that the information sent between customer browser and the Webserver cannot be read by others. Secure sessions allow determining the correct products and prices and when the customers purchase products.	***Rosesonly.com.au*** is a secured site using a VeriSign Digital Certificate. This ensures that all information will be encrypted. If any other user intercepts the communication, they will only be able to view an encrypted form. This makes it almost impossible to be intercepted by an unauthorised party. It explains that when the customers order on *rosesonly.com*, Firstly, a security notice will appear. Also, a secure icon will appear on the browser. For Microsoft Internet Explorer, a lock icon  and Netscape it is a key icon.  The Secure site can also be identified by the address. 'https://'. The industry standard for encryption technology, SSL is used which is compatible with Internet Explorer, Netscape and most other browsers.
Authority	Woolworths Limited http://www.homeshop.com.au/info/SecurityTechFAQ.asp	http://www.rosesonly.com.au/Security.asp#sec8
Currency	Last Updated: Monday, 20 September 2004	Current 2004 Roses Only
Scope	Covers most aspects of Security issues. Explains in detail the use of cookies and Java script.	Security and Privacy section highlights information about Collection and Use of information, cookies, privacy in emails, security and browsers.
Accuracy	For Questions or problems regarding Woolworths HomeShop, call customer representatives on 1300 666 377	www.rosesonly.com.au is a Verisign Secure site. Its validity period is from 06 Nov 03 –05 Nov 04 (checked on 22 Sep 2004)

6. CONCLUSION

The degree of satisfaction through online should be equal to the service they get in an offline environment. This paper addresses a need for a framework to better understand customers' online trust. The model reflects consumers' expectations. Businesses can develop e-business strategies to attract more customers through trust in their web sites. As a new form of conducting business over the Internet, e business involves uncertainty and risk than traditional way of doing business. It is obvious that all the businesses mentioned in this paper continue to maintain their eBusiness practices with superior quality, accuracy and currency. It can be concluded that each of the four businesses place major emphasis on their privacy and security policies. Each use the strongest form of SSL encryption (128-bit), which provides a very high level of protection against unauthorised access and prevent unauthorised persons from reading information customers send to the business, while it is in transit over the Internet. Ensuring security gives confidence and assurance to the customer for a safe transaction. In answering the question ***how can we best evaluate e-business information for security purposes?*** The above four examples from two major industries would provide some insight in finding information that could be trusted from eBusiness web sites. All these websites identify data security measures implemented and address issues of privacy. All the sites

offer considerable amount of customer advice and information on their methods of protection. Some of the sites mention possible instances of where data security could be breached and how to identify them (i.e. Fraud, hoax emails). The banking industries have shown they have highlighted strongly on the issues of security and protecting of customers privacy. This is mainly due to the fact they are dealing with valuable assets and are needed to reassure customers, especially potential clients who will be investing through their banking system.

REFERENCES

[1].http://www.idc.com.au/resources/press/software/20021105_Security.htm
[2].www.anz.com.au
[3].http://www.telstra.com.au/ordering/tour/security.htm
[4].http://www.ozweb.biz/home_internetusage.html
[5].http://www.nua.com/surveys/index
[6].http://www1.ap.dell.com/content/topics/topic.aspx/ap/policy/en/privacy?
[7].http://telstra.com/hosting/products/security/
[8].http://www.stgeorge.com.au/
[9].http://www.abs.gov.au
[10].www2.dcita.gov.au/publications/2004/01/scope/e-service